DOI: 10.2195/lj_Proc_schier_de_201610_01
URN: urn:nbn:de:0009-14-44770

Graph-basierte Privacy-orientierte Optimierung von Geschäftsprozessmodellen

Graph-based privacy-orientated optimization of business process models

***Arkadius Schier*[1]**
***Lucas Petrich*[1]**
***Michael ten Hompel*[1]**
***Björn Schwarzbach*[2]**
***Bogdan Franczyk*[2]**

[1] *Fraunhofer-Institut für Materialfluss und Logistik IML*

[2] *Universität Leipzig*

Mit der herausragenden Effizienz und dem allgemeinen Erfolg des Cloud-Computings sind Cloud-Innovationen ein alltäglicher Bestandteil der Industrie geworden. Besondere Bedeutung gewinnen darin Cloud-gestützte Geschäftsprozesse, welche dynamisch, als direkte Reaktion auf einen Kundenauftrag, angepasst und ausgeführt werden können. Gerade durch die Cloud-Basis wird dies für kooperative und interindustrielle Anwendungen genutzt. Dabei gewinnen unter der Kontrolle der Kollaborationspartner Privacy-Anforderungen im Sinne des Datenschutzes sowie Datensicherheits- und Vertraulichkeitsanforderungen erheblich an Wert. Gegenstand dieses Artikels ist die Erweiterung des Konzeptes und der Architektur einer zentralen Cloud-Plattform zur Konfiguration, Ausführung und Überwachung von kollaborativen Logistik-Prozessen. Auf dieser Plattform können Geschäftsprozesse modelliert und in ihren Privacy-Eigenschaften parametrisiert werden. Ein Schwerpunkt wird dabei auf die optimale Bestimmung eines Prozessflusses unter besonderer Berücksichtigung von Privacy-Anforderungen sowie ökologischer und ökonomischer Kosten gelegt. Dieser Prozessfluss wird daraufhin einem Nutzer der Plattform gemäß zuvor festgelegter Prioritäten vorgeschlagen.

[Schlüsselwörter: Management, Cloud, Logistik, Privacy, Organisation und Betrieb]

Because of the outstanding efficiency and the overall success of cloud computing, cloud innovations have become an everyday part of the industry. Cloud-based business processes, which can be dynamically, in direct response to a customer order, adjusted and executed, are of particular importance. These are used for cooperative and inter-industrial applications straight through the cloud-base. Privacy requirements in terms of data protection, data security and confidentiality requirements are gaining considerably in value under the control of the collaboration-partner. Subject of this article is the extension of the concept and the architecture of a central cloud platform for the design, execution and monitoring of collaborative logistics processes. On this platform, business processes can be modeled and parameterized in their privacy properties. An emphasis is placed on the optimal determination of a process flow with special consideration of privacy requirements and environmental and economic costs. This process flow is then proposed for a user of that platform in accordance with predetermined priorities.

[Keywords: Management, Cloud, Logistics, Privacy, Organization and Enterprise]

1 EINFÜHRUNG

Cloud Computing ist nicht nur äußerst erfolgreich, sondern findet mittlerweile in fast allen Industriezweigen Anwendung [WR]. In der Logistik zeichnet sich Cloud-Computing besonders mit seiner Dynamik, der dezentralen Verteilung, der Abstraktion von physischen Systemen und der schnellen Interaktion aus. Besondere Bedeutung gewinnt diese Systematik in der Logistik für Supply-Chains, bei welchen es häufig der Fall ist, dass diese aus mehreren Beteiligten bestehen und somit eine Kollaboration unumgänglich ist. Die Kollaboration wird von den Beteiligten organisiert und durch das gezielte Outsourcing und das Zusammenfließen gemeinsamen Wissens ergibt sich eine Mehrzahl an Vorteilen, welche für die Effizienzsteigerung der Supply-Chain förderlich ist.

Das genannte Management der Kollaboration in der Cloud auszuführen ist im Zuge der vierten industriellen Revolution ein notwendiger Fortschritt. Alle Partizipierende kommen einfach und schnell an die für sie benötigten Informationen und die eigenen zur Verfügung gestellten Dienste können direkt miteinander verbunden und kombiniert werden. Ein solches zentrales Management

DOI: 10.2195/lj_Proc_schier_de_201610_01
URN: urn:nbn:de:0009-14-44770

inklusive der Dynamik dieses Systems schafft die Möglichkeit Kundenaufträge angepasst und effizient auszuführen. Ein Gesamtprozess innerhalb einer Supply-Chain existiert somit durch eine Verkettung von IT-Diensten verschiedenster Partner, welche miteinander kooperieren. Der im System integrierte Dienst eines Partners wird dabei jedoch in der Cloud-Umgebung des Partners unter der lokalen Kontrolle ausgeführt. Dies bezeichnet man als Collaborative Business Process-as-a-Service (Collaborative BPaaS). Privacy im Sinne des Datenschutzes, Datensicherheits- und Vertraulichkeitsanforderungen sind aufgrund des hohen Datenaustausches innerhalb eines Gesamtprozesses zwischen verschiedenen, möglicherweise internationalen Partnern keine geringfügige Anforderung, sondern ein entscheidender Faktor für den Erfolg der Zusammenarbeit. Cloud-Provider haben bei einem Collaborative BPaaS die Verpflichtung die empfangen, erzeugten und gesendeten Daten vertraulich zu behandeln und nur gemäß den Privacy-Präferenzen des Daten-Eigentümers bzw. Dienstnutzers zu speichern oder an weitere Dienste bzw. Provider zu übermitteln.

Die Zusammenarbeit der Dienste der jeweiligen lokalen Cloud und die Ausführung des Gesamtprozesses auf einer zentralen Plattform inklusive des zugehörigen Datenaustausches sowie der Zugriffskontrolle müssen exakt und fein-granular geregelt sein. Wenn dies gegeben ist, kann ein hohes Niveau an Privacy im Sinne des Datenschutzes sowie Datensicherheits- und Vertraulichkeitsanforderungen gewährleistet sein. Nicht nur die Vertraulichkeit im Umgang mit Geschäftsdaten ist erforderlich, sondern auch eine Sparsamkeit im Versand von Geschäftsdaten. Es sollten lediglich so viele wie nötig, aber so wenige wie möglich ausgetauscht werden. Zur Umsetzung, Kontrolle und Zertifizierung dieser Anforderungen ist eine einheitliche, zentrale Definition von Privacy-Anforderungen für den Umgang der jeweiligen Geschäftsdaten mit Bezug auf die involvierten IT-Dienste eines Gesamtprozesses eine notwendige Voraussetzung. Dafür ist eine zentrale Cloud-Plattform zur Konfiguration, Ausführung und Überwachung kollaborativer Geschäftsprozesse notwendig, welche durch PREsTiGE gegeben ist. Durch diese Plattform können Logistik-Prozesse modelliert und ihre Privacy-Eigenschaften parametrisiert werden. Somit können die einzelnen Prozesselemente mit externen cloudbasierten IT-Services unter Berücksichtigung der konfigurierten Privacy-Anforderungen verknüpft werden.

Mit den Industriepartnern Zimory GmbH Berlin, Salt Solutions GmbH und PSI Logistics GmbH arbeitet das Institut für Wirtschaftsinformatik der Universität Leipzig, das Forschungszentrum FZID der Universität Hohenheim und das Fraunhofer-Institut für Materialfluss und Logistik IML in Dortmund zusammen im vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Projekt PREsTiGE (Privacy-erhaltende Methoden und Werkzeuge für Cloud-basierte Geschäftsprozesse) an der Entwicklung von Methoden und Werkzeugen zur Privacy-Erhaltung im Geschäftsmodell Collaborative Business-Process-as-a-Service (BPaaS). Als Zielgruppenkontakt wird mit dem Staatsbetrieb Sächsische Informatik Dienste in Dresden und der AHP GmbH & Co. KG in Berlin kooperiert. PREsTiGE adressiert die Privacy-Erhaltung insbesondere in kollaborativen Cloud-basierten Geschäftsprozessen, in denen ein Prozess nur eingeschränkt zentral ausgeführt wird. Eine Architektur und ein Konzept für eine PREsTiGE-Plattform wurde erstmalig in [SSP+15] betrachtet und wird im dritten Kapitelerläutert.

Durch eine Mehrzahl an Service-Providern (Dienstleistern) ergibt sich eine Diversität in der Einhaltung von verschiedenen Privacy-Anforderungen bei vergleichbaren Services. Diese Diversität ergibt sich für den Service eines jeweiligen Providers in unterschiedlichem Wert. Weiterhin ist der Service durch wirtschaftlichen und ökologischen Wert zu betrachten. Ein Fokus dieses Artikels liegt in der Betrachtung der Definition verschiedener Privacy-Anforderungen, deren Wert und einer Gewichtung derer gegenüber des wirtschaftlichen und ökologischen Wertes eines Service sowie zueinander. Auf Basis dessen soll die Plattform PREsTiGE erweitertet werden, sodass bei einer Vielzahl an einzelnen Prozessen innerhalb eines Gesamtprozesses der optimale Prozessfluss anhand eigener Präferenzen bestimmt werden kann.

Der Artikel gliedert sich wie folgt. Das zweite Kapitel beschreibt den aktuellen Stand der Wissenschaft und der Technik in Bezug auf Cloud-Computing und Privacy. Im dritten Kapitel folgt die Beschreibung des Konzeptes und der Architektur für die zentrale Cloud-Plattform PREsTiGE. Den Schwerpunkt des Artikels bildet das vierte Kapitel, das auf die Bestimmung eines optimalen Prozessflusses innerhalb eines Geschäftsprozesses eingeht. Hier wird eine Gewichtung zwischen ökologischen, ökonomischen und Privacy-Kosten geschaffen und auf Basis dessen ein Optimum des Prozessflusses bestimmt. Dies wird an einem Beispiel evaluiert. Den Abschluss bildet das fünfte Kapitel, welches einen Ausblick auf die weiteren Arbeiten gibt.

2 Stand der Wissenschaft und Technik

2.1 Cloud Computing

Folgt man dem Bundesamt für Sicherheit in der Informationstechnik [BU12] versteht man unter Cloud-Computing das „das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die Spannbreite der im Rahmen von Cloud-Computing angebotenen Dienstleistungen umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur (z. B.

DOI: 10.2195/lj_Proc_schier_de_201610_01
URN: urn:nbn:de:0009-14-44770

Rechenleistung, Speicherplatz), Plattformen und Software."

Eine serviceorientierte Architektur (SOA) ist eine der Grundvoraussetzungen für Cloud Computing [BU12]. Zudem sollte eine Umgebung der Cloud mandantentauglich sein, da sich viele Nutzer gemeinsame Ressourcen teilen. Im Allgemeinen wird dies in dem Rahmen XaaS (Everything as a Service) in drei Modelle [NI11a] aufgeteilt, nach welchen Cloud-Computing angewandt wird:

- *Infrastructure as a Service (IaaS):* Rechenleistung und Speicherkapazitäten wird über das Internet bereitgestellt.
- *Platform as a Service (PaaS):* Laufzeiten bzw. Entwicklungsumgebung als Dienstleistung sind über das Internet zur Verfügung gestellt.
- *Software as a Service (SaaS):* Die Software selbst wird als Dienstleistung über das Internet distribuiert.

Um logische Ressourcen von den physischen Ressourcen zu abstrahieren und somit die zuvor beschriebenen wesentlichen Charakteristiken des Cloud Computing, finden verschiedene Formen der Virtualisierung ihre Anwendung [RCL09]. Durch die Virtualisierung von Netzwerken, Servern und Speichern können somit IT-Umgebungen verschiedener Arten dynamisch realisiert, in ihrer Größe angepasst und allokiert werden. Dadurch wird ein wesentlicher Beitrag zur Skalierbarkeit, Kostenkontrolle und Agilität getragen.

Durch die Integration unterschiedlicher Applikationen wird keine Problematik mit Schnittstellen geschaffen und eine kurzfristige Nutzung ermöglicht, da die Konfiguration und Provisionierung durch eine webbasierte Benutzungsschnittstelle durch den Nutzer selbst erfolgen kann und somit nur eine sehr geringfügige bis zu keiner Interaktion mit dem Provider erforderlich ist. Die Komplexität eines solchen, geteilten Systems steigt jedoch dennoch mit der Nutzeranzahl und der Anzahl der miteinander in Verbindungen stehenden Services. Subjektiv betrachtet kann der Eindruck eines Kontrollverlustes entstehen, da durch die Abstraktion und die dynamische Verteilung vor Ressourcen subjektiv nicht mehr ermessen werden kann, wo die Daten gespeichert werden oder welche Kommunikationskanäle diese beim Austausch nutzen. Dem zuvorkommend haben sich bereits mehrere Dienstleistungen im Bereich der Cloud-Computing entwickelt, welche die Datenverarbeitung und -speicherung unter nationalen Grenzen gewährleisten wollen [BU08].

Der juristische Rahmen des Cloud Computing ist selten eindeutig und klar, da die Haftungsbedingungen eines Providers von den zu erfüllenden und zuvor bestimmten Leistungspflichten abhängig sind [WE13]. Durch den internationalen Charakter der verteilten Systeme nimmt die Bedeutung dieses juristisch jungen und noch umstrittenen Bereiches zu. In [WE13] wird die offene Frage gestellt, ob Daten schutzfähig sind und unter welchen Bedingungen ein Schutz überhaupt möglich ist, wenn diese nicht einzelnen physischen Datenträgern exakt zugewiesen werden können.

Gemäß der Sicherheitsempfehlungen für Cloud Computing Anbieter [BU12] des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sollen Standards geschaffen werden, um die Sicherheit von Cloud Computing Plattformen überprüfbar zu gestalten. Dabei sind Vertraulichkeit und Verfügbarkeit als Grundwerte zu schützen sowie die Sicherheit der Rechenzentren nach aktuellem Stand der Technik zu gewährleisten. Durch eine Verschlüsselung wird dabei eine Sicherheit der Kommunikation sicherzustellen. Das Management der kryptographischen Dienste und Schlüssel erweist sich jedoch als komplex und durch einen Mangel der entsprechenden Werkzeuge als kaum umgesetzt. Wie in [JÄ15] beschrieben ist bspw. der PGP-Standard zur Mail-Verschlüsselung „hochsicher, kaum genutzt und völlig veraltet". Technisch betrachtet handelt es sich um eine „großartige" Lösung, doch die Nutzung ist schwierig und kompliziert.

2.2 PRIVACY

Die weiteste Fassung von Privacy ist in den Menschrechten der vereinten Nationen verankert [Ve48], dennoch ist die Definition des Begriffes selbst nicht trivial. Es existieren unterschiedliche Formen und Anwendungsgebiete von Privacy, zum Beispiel das Recht „allein gelassen zu werden" oder das Recht „Informationen über sich selbst zu kontrollieren".

Innerhalb der EU wurde 1995 die Richtlinie 95/46/EG des europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr definiert [EU95]. Eine Neufassung dieses Gesetzes wurde am 4. Mai 2016 unter dem Namen *General Data Protection Regulation (GDPR)* [Co16] veröffentlicht. Die in ihr enthaltenden gesetzlichen Regelungen treten ab dem 25. Mai 2018 in Kraft. In Deutschland wird die bisherige Fassung durch das Bundesdatenschutzgesetz in seiner Neufassung von 2003 umgesetzt [Bu90]. Gemäß dem Electronic Privacy Information Center (EPIC) [JB05] ist „Datenschutz weitestgehend zu verstehen, als das Recht eines Individuums die Sammlung, Nutzung und Verbreitung seiner personenbezogenen Informationen, welche von anderen gehalten werden, zu kontrollieren".

In der Richtlinie 95/46/EG des europäischen Parlaments und des Rates [EU95] sind personenbezogene Informationen (engl. Personally Identifiable Information (PII)) definiert als „alle Informationen über eine bestimmte oder bestimmbare natürliche Person („betroffene Person"); als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem

DOI: 10.2195/lj_Proc_schier_de_201610_01
URN: urn:nbn:de:0009-14-44770

oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind.“ Dies ist in weiteren, aktuelleren Definitionen [MI08] erweitert worden um „sensible PII, welche so wichtig für das Individuum sind, dass diese Informationen eines speziellen Schutzes benötigen.“

Für Unternehmen ist Privacy ein essentielles Thema im Kontext von Regelkonformität und Geschäftsrisiko [PC09]. Die Vorteile des Cloud-Computing – die schnelle Skalierbarkeit, Fernspeicherung von Daten und dem Verbreiten von Services in einer dynamischen Umgebung - können zu Nachteilen für den Erhalt eines Privacy-Niveaus werden. Dies könnte zum Beispiel dennoch notwendig sein, um nicht nur juristischen Gesetzgebungen gerecht zu werden, sondern auch um das Vertrauen potentieller und bestehender Kunden zu erhalten.

Um Organisationen bei der Einhaltung von Privacy-Regulatorien zur Seite zu stehen und diese zunehmend zu verpflichten, haben sich Vereinigungen gegründet und Privacy-Anforderungen an neue und bestehende Systeme formuliert. Zum Beispiel wurde im November 2007 vom UK Information Commissioners Office (ICO) ein „Privacy Impact Assessment (PIA) Prozess“ zur Verfügung gestellt, um Organisationen bei der Beurteilung des Einflusses ihrer Operationen auf den eigenen Datenschutz zu bewerten [PE09]. Das Unternehmen Microsoft hat im Jahr 2008 „Privacy Guidelines for Developing Software Products and Services“ veröffentlicht [MI08], um die Einhaltung von Datenschutz bei der Entwicklung neuer Software maßgeblich zu unterstützen. Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) hat im Jahr 2011 eine „PIA Guideline for RFID Applications“ [BU11] veröffentlicht, um Datenschutz-Risiken und deren Kontrolle in Bezug auf RFID-Anwendungen zu adressieren. Im Jahr 2011 hat das National Institute of Standard and Technology (NIST) „Guidelines for Security and Privacy in Public Cloud Computing“ veröffentlicht [NI11b].

Privacy-by-Design ist ein Grundsatz, welcher bei der Entwicklung neuer Systeme notwendig erscheint, aber nach Stahl und Burgmair [SB15] „vor allem bei Datenschützern als ideales Gestaltungsprinzip gilt. Doch konkrete Umsetzungshinweise und Anregungen für Entwickler gibt es nicht“. Den aktuellen Stand der Forschung im Bereich von Datenschutz im Cloud-Computing beschreiben Itani et al. [IKA+09] folgendermaßen:

“Research on data privacy in cloud computing is still in its early stages.”

Wörtlich übersetzt bedeutet dies, dass *„sich die Forschung über den Datenschutz im Cloud-Computing noch in einem frühen Stadium befindet."* Zu gleichen Aussagen kommen Pearson et al. [PC09] und Zhan et. al. [ZYZ+12] in ihren Artikeln. Hier beschreiben die Autoren, dass Datenschutz im Cloud-Computing von Bedeutung ist, jedoch die Problematik noch ungelöst ist oder sich noch im Anfangsstadium befindet.

3 KONZEPT UND ARCHITEKTUR DER KOLLABORATIVEN CLOUD-PLATTFORM

In diesem Kapitel werden das Konzept und die Architektur für eine zentrale Cloud-Plattform zur Konfiguration, Ausführung und Überwachung von kollaborativen Logistik-Prozessen dargestellt, welche erstmalig in [SSP+15] beschrieben wurden. Die Architektur gliedert sich, wie in Abbildung 1 ersichtlich ist, in die drei Abschnitte: Die PREsTiGE Plattform, mehrere Gateways und verschiedene Dienst-Provider. Die PREsTiGE Plattform selbst ist aus den Modulen Konfigurator, Cockpit, Zertifizierung, Privacy-Management, Service Repository, Business Process Management System (BPMS) und Identity and Access Management System (IAMS) aufgebaut. Das IAMS [SPS+15] beantwortet Zugriffsanfragen durch die Auswertung der vom Privacy Management vorgegebenen Privacy-Anforderungen. Im Cockpit werden der aktuelle Stand der Ausführung eines Prozesses sowie eventuell entstandene Privacy-Verletzungen visuell dargestellt.

Die jeweiligen Provider können ihre Services, welche sie in ihrer jeweiligen lokalen Cloud-Plattform ausführen über ein Human Interface (HI) des Service-Repositories in die PREsTiGE-Plattform zur weiteren Überprüfung und Verwaltung eingepflegt werden. Dabei werden die angegebenen Dienst-Beschreibungen auf ihre Validität überprüft und anschließend übernommen.

Somit stehen diese Services den Nutzern in der PREsTiGE-Plattform zur Verfügung, welche dann im Konfigurator von dem Nutzer bei der Modellierung seines Geschäftsprozesses abrufen und einbauen kann.

Während dieser Modellierungsphase können Privacy-Anforderungen und –regeln, wie bereits von Schier et al. [SPS+15] beschrieben mithilfe des Privacy-Managements für einzelne Prozesse definiert werden. Diese werden daraufhin mit den zur Verfügung stehenden Diensten aus dem Service Repository abgeglichen. Existieren keine exakt auf die Anforderungen passende Dienste, wird dem Nutzer dies mitgeteilt und dieser kann die Privacy-Einstellungen anpassen oder sich um die Aufnahme passender Dienste kümmern. Um das Ausmaß dieses Kompromisses so gering wie möglich zu halten und genau abwägen zu können, wird einem im Konfigurator der Prozessfluss mit den geringsten Kosten vorgeschlagen, welcher den eigenen Prioritäten entspricht (siehe Kapitel 4). Nach der Modellierung des gesamten Collaborative BP-Diagrammes wird dieses bei Ausführbarkeit im Zertifizierungsmodul zertifiziert und anschließend dem Business Process Management System (BPMS) übergeben.

DOI: 10.2195/lj_Proc_schier_de_201610_01
URN: urn:nbn:de:0009-14-44770

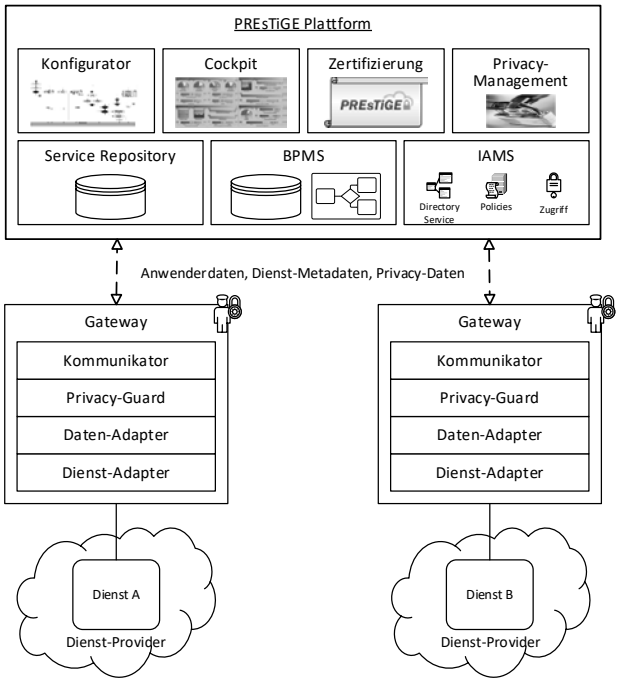

Abbildung 1. Architektur der kollaborativen Cloud-Plattform

Im BPMS können die zuvor modellierten Gesamtprozesse ausgeführt werden. Dabei wird für jeden einzelnen Prozess ein Gateway instanziiert (vgl. den mittleren Bereich der Abbildung 1), welcher für die Privacy-Einhaltung, die Interoperabilität und die Verschlüsselung der Kommunikation zuständig ist.

Ein PREsTiGE-Gateway enthält die Bestandteile Kommunikator, Privacy-Guard, Daten-Adapter und Dienst-Adapter und hat die Pflicht inne, nur die freigegebenen Daten zwischen der Cloud-Plattform und dem jeweiligen Service auszutauschen. Die genannte Instanz eines Gateways existiert parallel zum jeweiligen Service-Aufruf und endet auch mit diesem. Ein Kommunikator innerhalb eines Gateways dient der Kommunikation zwischen der PREsTiGE Plattform und dem Service-zugehörigen Gateway. Der Privacy-Guard überprüft den Informationsfluss gemäß den zuvor festgelegten Privacy-Anforderungen und besitzt die Funktionalität gewisse Daten zu pseudonymisieren oder anonymisieren. Dadurch ist Informationsfluss nur mit Daten hergestellt, welche für den jeweiligen Service von absoluter Notwendigkeit sind. Der Daten-Adapter überführt das Domänen-Datenschema der PREsTiGE-Plattform in das Dienst-Datenschema und umgekehrt. Dieses Schema wird für den Austausch von Daten innerhalb der kollaborativen Plattform verwendet. Die Aufgabe des Daten-Adapters ist zudem der Kontakt des benötigten Dienstproviders über das Integrated Database Management System (IDMS) und der Erhalt der Ergebnisse dieser Anfrage. Die eingehenden Daten werden wieder in das Plattform-spezifische Domänen-Datenschema überführt. Nach der abgeschlossenen Kommunikation eines Service mit dem Provider wird die zugehörige Gateway-Instanz beendet, wodurch sich Gateways als kurzlebig erweisen und nur gemäß jedem Service-Aufruf existieren.

4 PRIVACY-ORIENTIERTE OPTIMIERUNG

In diesem Kapitel wird die Graph-basierte Optimierung von Geschäftsprozessen als Schwerpunkt des Artikels behandelt. Als Grundlage werden ökologische und ökonomische Kosten definiert sowie zwei Privacy-Faktoren als weitere Kosten betrachtet. Diese werden dann gebündelt für jeden Prozess eines Gesamtprozesses angewendet und in ein Geschäftsprozessdiagram integriert. Dieses wird daraufhin in einen Graphen umgewandelt, um in diesem einen optimalen Prozessfluss bestimmen zu können, welcher an den Prioritäten und Bedürfnissen des ausführenden Kunden angepasst ist. Abschließend wird dieses Konzept anhand eines Anwendungsfalles evaluiert.

4.1 KOSTEN VON GESCHÄFTSPROZESSEN

Aus der Unternehmenssicht ist der Schutz von eigenen Geschäftsdaten in besonderer Hinsicht auf den Kunden stets von hoher Wichtigkeit. Bei fehlender Berücksichtigung können juristische Konsequenzen drohen sowie ein Vertrauensverlust bestehender und neuer Kunden entstehen [WR]. Um das Vertrauen zu erhalten und solche Konsequenzen vermeiden zu können ist eine Formalisierung von Privacy-Anforderungen ein essentieller Schritt, um den Kunden die Möglichkeit zu schaffen die eigenen Anforderungen eigenständig zu analysieren. Außerdem schafft dies selbstständig Transparenz und damit Vertrauen. In dem vom BMBF geförderten Forschungsprojekt PREsTiGE werden Privacy-Anforderungen bezeichnet als eine nichtformale Aussage über die Schutzbedürftigkeit von Daten. Dabei werden vier Arten von Privacy-Anforderungen unterschieden [SSP+15]: providerbezogene Privacy-Anforderung, prozessbezogene Privacy-Anforderung, aktivitätsbezogene Privacy-Anforderung und dienstbezogene Privacy-Anforderung.

Dieser Artikel bezieht sich auf die Kosten von prozessbezogenen Privacy-Anforderungen. Prozessbezogen ist die Privacy-Anforderung eines Providers, die für einen spezifischen Prozess gilt, zum Beispiel: „In dem Prozess *XYZ* darf das Asset ‚Artikelwert' nur gelesen werden von: *Versender* und *Empfänger* (d. h. bspw. nicht von *Spediteur 1 oder Spediteur 2*)." Es kann jedoch der Fall eintreten, dass für diese Anforderung, wie bereits zuvor angesprochen, kein zutreffender Prozess zur Auswahl steht oder man bereits einen Gesamtprozess in die PREsTiGE-Plattform importiert hat, auf Basis dessen man eine Auswahl des Prozessflusses treffen muss. In diesem genannten Beispiel könnten mehrere verschiedene Spediteure zur Auswahl stehen, welche eine unterschiedlich hohe Anzahl an Daten zur Ausführung benötigen. Dies bezeichnet man als Privacy-Kosten. Je mehr Daten von einem Service innerhalb eines Collaborative BP angefordert werden, umso

DOI: 10.2195/lj_Proc_schier_de_201610_01
URN: urn:nbn:de:0009-14-44770

mehr Kosten entstehen im Sinne der Preisgabe von Daten. Betrachtet man dies in numerischen Werten, wird der Wert eines Assets auf 1 festgelegt. Bei dem genannten Beispiel könnte der dem *Spediteur 1* zugehörige Service bspw. die Assets *Name, Anschrift* und *Telefonnummer* für eine Ausführbarkeit verlangen, der Service von *Spediteur 2* jedoch nur *Anschrift* und *Telefonnummer*. Dadurch ergibt sich für die Nutzung des Service von *Spediteur 1* Privacy-Kosten in diesem betrachteten Faktor von 3 und für die Nutzung des Service von *Spediteur 2* Kosten in Höhe von 2. Im weiteren Verlauf des Artikels werden diese Privacy-Kosten Daten-Kosten genannt.

Als weiterer Faktor für Privacy-Kosten betrachtet dieser Artikel den Standort der Datenverarbeitung und –speicherung. Wie im obig genannten Beispiel kann eine prozessbezogene Anforderung bestehen, dass die Daten von dem jeweiligen Prozess bspw. nur in Deutschland verarbeitet und gespeichert werden dürfen. Durch verschiedene Server-Standorte und Backup-Mechanismen kann dies jedoch nicht immer garantiert werden [JSW+15]. Somit sind Privacy-Kosten für die Datenverarbeitung im internationalen Rahmen festzulegen. Wenn man sich in diesem Beispiel auf Deutschland als Verarbeitungs- und speicherstandort festgelegt hat, dann werden für die Ausverlagerung in die Europäische Union numerische Privacy-Kosten in Höhe von 2 festgesetzt. Außerhalb der Europäischen Union, aber innerhalb von Europa werden Kosten von 5 festgesetzt. Außerhalb von Europa entstehen Privacy-Kosten von 10. Der Verbleib der Datenverarbeitung und –speicherung in Deutschland entspricht dabei keinen Privacy-Kosten, da der Anforderung gerecht wird, und somit den Kosten in Höhe von 0. Im weiteren Verlauf des Artikels werden diese Privacy-Kosten Standorts-Kosten genannt.

Die genannten Privacy-Kosten werden zu einem numerischen Wert aufaddiert. Bei den im Beispiel genannten Kosten für *Spediteur 1* ergeben sich somit bei Daten-Kosten in Höhe von 3 und einer Datenverarbeitung innerhalb der Europäischen Union Standort-Kosten in Höhe von 2, was einen gesamten numerischen Wert für die Privacy Kosten von 5 ergibt. Im Vergleich dazu ergeben sich für den *Spediteur 2* bei Daten-Kosten von 2 und Standort-Kosten von 5, da man in Europa, aber nicht der Europäischen Union die Daten verarbeitet, insgesamt Privacy-Kosten in Höhe von 7. Eine solche Addition von Kosten ist jedoch nur bei miteinander vergleichbaren Werten sinnvoll. Beim Vergleich von Datenmenge und Verarbeitungsstandort ist eine Vergleichbarkeit hergestellt, da ein Nutzer bspw. bereit wäre mehr Daten freizugeben, wenn diese nur im Inland verarbeitet werden. Ein Vertrauen zum Provider ist dabei jedoch unabdingbar und wird mit einem von PREsTiGE zertifizierten Service hergestellt.

Nicht vergleichbar mit Privacy-Kosten sind ökologische und ökonomische Kosten eines Service. Jeder Service in der PREsTiGE-Plattform steht für einen IT-Service in der lokalen Cloud eines Providers. Hinter diesem Service können vielfältige logistische Aktivitäten stehen wie bspw. der Transport, Lagerung oder Bereitstellung von Gütern, Personen, Informationen oder Energie [KR12]. Solche Aktivitäten erzeugen zuerst Kosten in ökonomischer und somit vielfältiger Form. Diese können Personalkosten, Mietkosten, Nutzungskosten und viele mehr beinhalten. In diesem Artikel wird dies als Betriebskosten, welche notwendig sind, um einen Service auszuführen, abstrahiert. In dem zuvor bereits genannten Beispiel von *Spediteur 1* kann der Transport von Gütern bspw. ökonomische Kosten in Höhe von 100 € entsprechen. Im Gegensatz dazu erzeugt der Service von *Spediteur 2* Kosten in Höhe von 70 €.

Weiterhin erzeugt die Ausführung der Services Kosten in ökologischer Form. Um die Gesamtheit dieser Kosten zu betrachten und dies nur im Beispiel des Transportes von Gütern, müsste nicht nur der Transportweg selbst betrachtet werden, sondern auch die Herstellung und Entsorgung von dabei zum Einsatz kommenden Verpackungsmaterialen sowie einen Anteil der Herstellung und Entsorgung sowie Wartung und Instandhaltung der Transportfahrzeuge, Umschlagsplätze, Transportwege und sogar das beteiligte Personal müsste anteilig betrachtet werden. Der Aufwand dies zu ermitteln ist um einiges höher als der Aufwand des Service im Allgemeinen, weshalb dieser Artikel die ökologischen Kosten in diesem Beispiel auf die anteilige CO_2-Produktion des Transportfahrzeuges abstrahiert. Würde das Transportfahrzeug elektrisch betrieben und die elektrische Energie dafür aus erneuerbaren Energiequellen bezogen, wären diese Kosten so gering, dass die Betrachtung von Herstellung, Betrieb und Entsorgung des Transportfahrzeuges wieder in Frage käme. Der Grenzwert für Nutzfahrzeuge in den USA [EP14] liegt seit 2014 bei maximal $82{,}1\ mg\frac{CO_2}{tkm}$. In dem zuvor genannten Beispiel produziert *Spediteur 1* während des Transportweges $0{,}3\ g\ CO_2$ während *Spediteur 2* $0{,}5\ g\ CO_2$ erzeugt.

4.2 Integration und Umwandlung von Geschäftsprozessen

Um die Privacy-Kosten, die ökonomischen Kosten und die ökologischen Kosten betrachten zu können, werden diese in das Collaborative BP-Diagram als Annotation zu den jeweiligen Services als Tupel integriert. Der Aufbau eines solchen besteht aus Privacy-Kosten (PK) und einem Gewichtungsfaktor p, ökonomischen Kosten (NK) und einem Gewichtungsfaktor n und ökologischen Kosten (LK) und einem Gewichtungsfaktor l. Dies ergibt ein Tupel wie folgt:

$$(p * PK, n * NK, l * LK)$$

Diese Kosten sind von den jeweiligen Providern der Services bei dem Importieren des Service in die PREsTiGE-Plattform einzutragen. Die Daten-Kosten werden da-

DOI: 10.2195/lj_Proc_schier_de_201610_01
URN: urn:nbn:de:0009-14-44770

bei automatisch bestimmt. Die Gewichtungsfaktoren p, n oder l sind daraufhin vom Nutzer des Gesamtprozesses festzulegen, um einen optimalen Prozessfluss nach seinen Bedürfnissen bestimmen zu können (siehe Kapitel 4.3).

In dem bereits zuvor genannten Beispiel entsteht somit für den Service von *Spediteur 1* das Tupel $(5p, 100n, 0{,}3l)$ und für den Service von *Spediteur 2* das Tupel $(7p, 70n, 0{,}5l)$. Diese Tupel sind an dem spezifischen Service im Collaborative BP-Diagramm annotiert, wobei die Gewichtungsfaktoren nutzerseitig festzulegen sind.

Zur Graph-basierten Verarbeitung des Collaborative BP-Diagrammes ist eine Transformation dessen in einen Graphen, wie in Tabelle 1 dargestellt, notwendig. Gemäß der Business Process Model and Notation (BPMN) besteht ein Geschäftsprozess aus mehreren Aktivitäten (engl. Activity), welche mithilfe von Sequenzflüssen (engl. Sequence Flows) mit Events oder Gateways verbunden sind. Eine Aktivität kann für einen Service (somit einzelnen Task) in der PREsTiGE-Plattform stehen oder einen Unterprozess abstrahieren. Dieser Artikel betrachtet als Events Start- und End-Events, welche den Beginn oder das Ende eines Geschäftsprozesses signalisieren. Als Gateways werden exklusive (XOR), inklusive (OR) und parallele (AND) Gateways betrachtet. Dabei sind divergierende Gateways, aus welchen mehrere Sequenzflüsse ausgehen von konvergierenden Gateways, welche mehrere Sequenzflüsse zu einem zusammenführen, zu unterscheiden.

Ein gerichteter, gewichteter Graph ist nach Brandstädt [BR94] ein Paar $G = (P, E)$, hierbei ist P eine endliche Menge von Knoten und E enthalten in $P\ x\ P$ eine Relation auf P, die geordnete Menge der gewichteten Kanten, wobei $e_{p_i,p_j} \in E$ eine Kante von Knoten $p_j \in P$ nach Knoten $p_i \in P$ ist. Dann ist der Knoten p_i der direkte Nachfolger vom Knoten p_j und der Knoten p_j der direkte Vorgänger vom Knoten p_i. Durch die zugehörig Kantengewichtsfunktion $d: E \to \mathbb{R}_+$ ist jeder Kante $e_{p_i,p_j} \in E$ das positive, reelle Tupel $d\left(e_{p_i,p_j}\right)$ zugeordnet.

Der Ausgangsgrad $out(p_j)$ eines Knotens p_j ist gleich der Anzahl seiner direkten Nachfolger: $out(p_j) = \left|\{p_i | (p_i, p_j) \in E\}\right|$ Der Eingangsgrad $in(p_i)$ eines Knotens p_i ist gleich der Anzahl seiner direkten Vorgänger: $in(p_i) = |\{p_j | (p_i, p_j) \in E\}|$. Der Graph enthält keine isolierten Knoten, wenn also für den Knoten $p\ out(p) = in(p)$ gilt, so gilt auch $out(p) = in(p) \geq 1$.

Der Knoten $p_s \in P$ entspricht dem Start-Event $E_s \in D$ innerhalb der Business Process Model and Notation (BPMN), welches den Anfang eines Business Process Diagram (BPD) D darstellt. Der Knoten $p_s \in P$ stellt somit den Startknoten des Graphs G dar mit $in(p_s) = 0$. Ein Knoten $p_i \in P$ entspricht einer Activity $A_i \in D$ innerhalb der BPMN, welche einen Service beschreibt, welcher in einem Geschäftsprozess ausgeführt wird. Eine gerichtete, gewichtete Kante $e_{p_i,p_j} \in E$ entspricht einem Sequenzfluss innerhalb der BPMN. Der Knoten $p_f \in P$ entspricht dem End-Event $E_f \in D$ innerhalb der BPMN, welches das Ende des BPD D darstellt. Der Knoten $p_f \in P$ stellt somit den Endknoten des Graphs G dar mit $out(p_f) = 0$. Das Gewicht $d\left(e_{p_i,p_j}\right)$ der Kante e_{p_i,p_j} entspricht den Kosten der Aktivität $A_j \in D$, welche durch den Ausgangsknoten p_j repräsentiert wird. In einem Collaborative BP-Diagramm repräsentiert eine Aktivität für die Ausführung eines Service. In einem Graphen repräsentiert ein Knoten einen Zustand und eine Kante für eine Zustandsänderung. Daher sind die Gewichtstupel an den Kanten anstelle der Knoten.

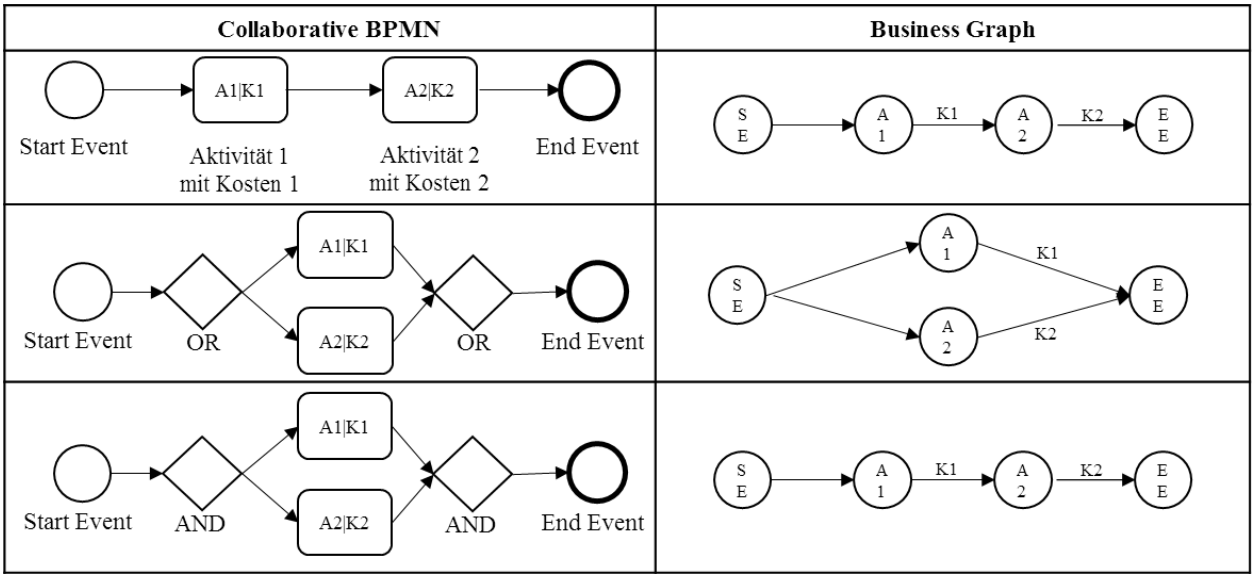

Tabelle 1. *Transformation von Collaborative BPMN zu Business Graph*

DOI: 10.2195/lj_Proc_schier_de_201610_01
URN: urn:nbn:de:0009-14-44770

Ein gerichteter Weg $W =< p_s, p_i, \dots, p_f >$ in dem gerichteten, gewichteten Graphen G bezeichnet eine Folge von Knoten $p_i \in P$ von einem Start-Knoten $p_s \in P$ zu einem Ziel-Knoten $p_f \in P$, welche jeweils durch aufeinander folgende, gerichtete, gewichtete Kanten miteinander verbunden sind. Das Gewicht des gerichteten Weges ist dabei die Summe der aufeinander folgenden, gerichteten, gewichteten Kanten von dem Start-Knoten $p_s \in P$ zu dem Ziel-Knoten $p_f \in P$:

$$d\left(W_{p_f,p_s}\right) = \sum_{i=s,\ j=Nachfolger(s)}^{f,\ Vorgänger(f)} d(e_{p_i,p_j})$$

Ein günstigster, gerichteter Weg W in einem gerichteten, gewichteten Graphen wäre eine Folge von Knoten $p_i \in P$ von einem Start-Knoten $p_s \in P$ zu einem Ziel-Knoten $p_f \in P$, welche jeweils durch aufeinander folgende, gerichtete, gewichtete Kanten miteinander verbunden seien, bei der das Gewicht des gerichteten Weges $d\left(W_{p_f,p_s}\right)\ minimal$ wäre. Das bedeutet es gäbe keinen anderen Weg mit geringerem Gewicht und es gäbe höchstens einen oder mehrere Wege mit gleichem Gewicht. In diesem Artikel trifft dies jedoch nicht direkt zu, da Tupel mit nicht vergleichbaren Werten nicht in sich aufaddiert werden können, sondern als Tupel bestehen bleiben und nur lediglich Tupel mit Tupel aufaddiert werden. Daher ist es nötig ein Pareto-Optimum zu bestimmen (siehe Kapitel 4.3).

Exklusive (XOR) und inklusive (OR) Gateways werden in dem Graphen zu Kanten umgewandelt. Dabei werden alle eingehenden und ausgehenden Sequenzflüssen eines Gateways miteinander kombiniert, wodurch Kanten von den zuvor ausgehenden Knoten mit den nachfolgenden Knoten des Gateways verbunden werden. Für die Graph-basierte Optimierung ist diese Generierung von mehr Kanten gestattet [BJR00], da es gemäß dem Gateway ausreicht (OR) oder nur gestattet ist (XOR) einen einzigen Weg zu beschreiten. Dies wird in Zeile 2 der Tabelle 1 dargestellt. In der linken Spalte ist in der Business Process Modeling Notation (BPMN) abgebildet, welche einen Prozess aus einem Start- und End-Event sowie zweier OR-Gateways und zweier Aktivitäten A1 und A2 mit den jeweiligen Kosten K1 und K2 darstellt. Auf der rechten Seite der Tabelle 1 ist der transformierte Business Graph dargestellt. Es ist zu erkennen, dass der Sequenzfluss vom Start-Event zur Aktivität 1 über den divergierenden OR-Gateway zu einer direkten Kante zu Aktivität 1 umgewandelt wurde. Selbiges wurde mit dem Sequenzfluss vom Start-Event zur Aktivität 2 durchgeführt. Ebenso wurden die Sequenzflüsse des konvergierenden OR-Gateways in direkte Kanten zur nachfolgenden Aktivität umgewandelt. Eine analoge Verfahrensweise findet mit XOR-Gateways statt.

Bei einem parallelen Gateway (AND) ist bei der Transformation in einen Graphen sicherzustellen, dass beide ehemaligen Sequenzflüsse bei der Optimierung durchlaufen werden. Dies erfordert eine Umstrukturierung des Collaborative BP-Diagrammes dahingehend, dass die parallel auszuführenden Aktivitäten nacheinander im Graph miteinander verbunden werden. Dadurch werden bei der Optimierung beide Knoten oder Knotenfolgen nacheinander durchlaufen, um die Kosten dieser zusammen berücksichtigen zu können. Wie in der dritten Zeile der Tabelle 1 zu erkennen ist, wird der parallele Sequenzfluss des Collaborative BPMN in einen seriellen Ablauf im Graphen transformiert. Die Aktivität 1 und 2 werden dadurch nicht parallel ausgeführt, sondern hintereinander, um die Betrachtung der Kosten der beiden, einst parallelen Wege in der Optimierung garantieren zu können.

4.3 Bestimmung eines optimalen Prozessflusses

Für den vorliegenden Graphen, welcher durch die Transformation des Collaborative BP-Diagrammes generiert wurde, ist nun ein Pareto-optimaler Weg zu bestimmen. Ein Pareto-Optimum beschreibt einen Zustand, in welchem es nicht möglich ist, eine Eigenschaft (in diesem Fall ökologische, ökonomische oder Kosten der Privacy) zu verbessern ohne gleichzeitig eine andere zu verschlechtern. Für jede Kante e_{p_i,p_j} des Graphen ist ein dreidimensionales Tupel $d\left(e_{p_i,p_j}\right) = (p * PK_j, n * NK_j, l * LK_j)$ als Gewichtungsfunktion gegeben. Dieser Artikel nimmt der Einfachheit halber an, dass sich die Kosten des Weges W durch die Addition aller Tupel der Kanten des Weges W ergeben (siehe Kapitel 4.2). Nach Möhring [MÖ99] ergeben sich jedoch bei diesem mehrkriteriellen Kürzeste-Wege-Problem, welches sich mit einer einfachen Erweiterung des Dijkstra-Algorithmus berechnen lässt [JA84], mehrere Pareto-optimale Wege und somit Lösungen. Bei n Knoten werden somit 2^{n-1} Pareto-optimale Lösungen erzeugt, wenn man alle Lösungen berechnen möchte. Durch diese exponentielle Steigerung ist die Bestimmung aller Pareto-optimaler Lösungen schwach NP-schwer. Aufgrund dessen findet eine Approximation der Pareto-optimalen Wege nach Warburton [WA87] durch eine Gewichtung der Summe der Kriterien durch die Gewichtungsfaktoren p, n und l statt. Der Nutzer des Gesamtprozesses legt im Konfigurator der PREsTiGE-Plattform fest, welche Werte W_n, W_p oder W_l für die einzelnen Kosten nicht überschritten werden dürfen. Durch diese Obergrenzen werden geeignete Gewichtungsfaktoren für die ökonomischen Kosten (Faktor n), Privacy-Kosten (Faktor p) und die ökologischen Kosten (Faktor l) bestimmt. Stellt der Nutzer keine Obergrenzen oder diese nur vereinzelt ein, stehen die übrigen Faktoren auf dem Wert 1.

Dadurch wird eine Näherungslösung nach den Bedürfnissen des Nutzers bestimmt und diese dem Nutzer visuell präsentiert für die ihm optimalste Möglichkeit eines Prozessflusses. Gemäß dieser Empfehlung des Konfi-

DOI: 10.2195/lj_Proc_schier_de_201610_01
URN: urn:nbn:de:0009-14-44770

gurators kann der Nutzer dieser folgen und seinen Gesamtprozess anpassen. Trifft die Empfehlung nicht mit seinen Anforderungen zusammen, ändern sich die Anforderungen oder stehen neue Services zur Verfügung bzw. bestehende Services nicht mehr zur Verfügung, so werden neue Empfehlungen generiert oder der Nutzer hat die Möglichkeit seine Grenzen anzupassen.

4.4 Evaluation

In diesem Unterkapitel wird das zuvor beschriebene Konzept der Optimierung anhand eines Anwendungsfall aus dem Forschungsprojekt PREsTiGE evaluiert.

In Abbildung 2 ist der Anwendungsfall in der Business Process Modeling Notation (BPMN) gegeben. Dieses beschreibt eine einfache logistische Operation in Form des Versendens von Gütern über zwei verschiedene Spediteure und einem Hub zum Sendungsumschlag. Wie anhand der XOR-Gateways erkenntlich ist, kann der Transport der Sendung zum Hub oder zum Empfänger nur von einem Spediteur durchgeführt werden. Der Transport zum Hub kann von drei Spediteuren ausgeführt werden, der Transport zum Empfänger von zweien. Parallel zum Transport zum Empfänger muss dieser benachrichtigt werden. Die in Kapitel 4.1 definierten Kosten der einzelnen Prozesse sind in den rot dargestellten Tupel visualisiert. In der Form $(p * PK, n * NK, l * LK)$ symbolisiert PK die Privacy-Kosten, NK die ökonomischen Kosten und LK die ökologischen Kosten. p, n und l dienen dabei als Gewichtungsfaktoren, welche in der allgemeinen Bestimmung eines Pareto-Optimum nicht zu beachten sind.

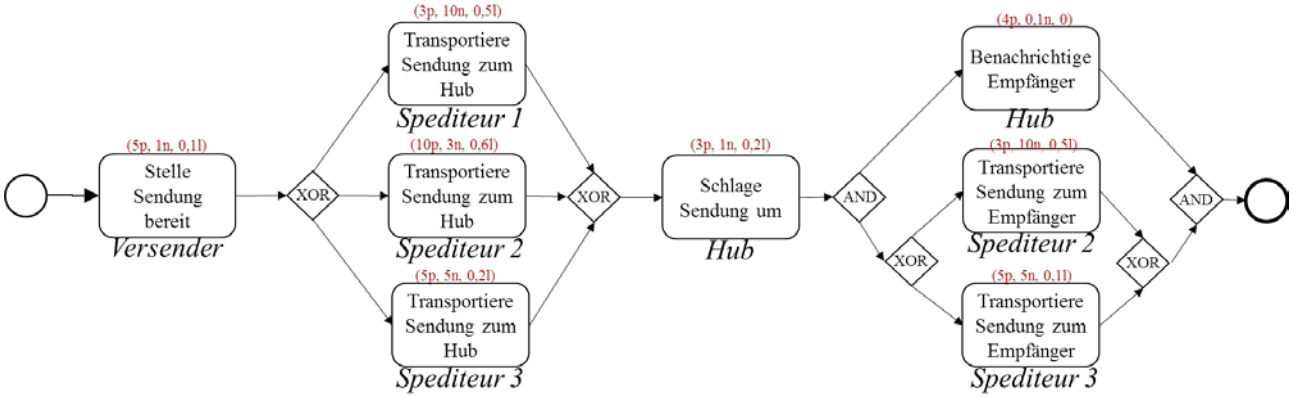

Abbildung 2. PREsTiGE-Anwendungsfall in Business Process Modeling Notation

Nun wird dieser Gesamtprozess in BPMN in einen Business Graphen gemäß der Beschreibung in Kapitel 4.2 transformiert. Der dabei generierte Business Graph ist in Abbildung 3 dargestellt. Wie zuvor beschrieben sind die Kosten nun an den nachfolgenden Kanten notiert und ebenfalls rot eingefärbt. Nun gilt es die jeweiligen Pareto-Optima allgemein zu bestimmen, wie in Kapitel 4.3 beschrieben wurde.

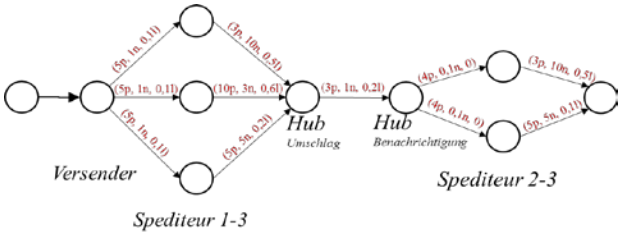

Abbildung 3. Abbildung 3: PREsTiGE-Anwendungsfall als Business Graph

In Tabelle 2 sind alle Pareto-Optima des Graphen aus Abbildung 3 dargestellt. Eine Spalte zeigt dabei die aktuellen Optima beim Erreichen des jeweiligen Knotens. Durch die Auswahl an Spediteur 1-3 entstehen dabei drei verschiedene Optima und bei der weiteren Auswahl zwischen den Spediteuren 2 und 3 entstehen sechs verschiedene Optima. Jedes Pareto-Optimum entsteht durch einen Prozessfluss innerhalb des Business Graphen. Das für den Nutzer passende Optimum ist nun von dessen Anforderungen abhängig. Möchte dieser seine Privacy-Kosten möglichst gering halten und setzt als oberen Wert 20 für diese Kosten an, so wäre das dritte Pareto-Optimum der Tabelle 2 für ihn optimal (20p, 17,1n, 1l), da die ökonomischen und ökologischen Kosten in diesem Pareto-Optimum geringer sind als die des ersten Optimums (19p, 22,1n, 1,3l) und die Anforderung an die Privacy-Kosten erfüllt bleibt. Überträgt man dies auf den PREsTiGE-Anwendungsfall in der BPMN, so ergibt sich die Empfehlung für die Wahl des Spediteurs 3 für den Transport zum Hub und den Spediteur 2 für den Transport zum Empfänger.

Versender	Spediteur 1-3	Hub (Umschlag)	Hub (Benachrichtigung)	Spediteur 2-3	Ende
(0,0,0)	(5p, 1n, 0,1l)	(8p, 11n, 0,6l) (15p, 4n, 0,7l) (10p, 6n, 0,3l)	(12p, 12n, 0,8l) (18p, 5n, 0,9l) (13p, 7n, 0,5l)	(16p, 12,1n, 0,8l) (22p, 5,1n, 0,9l) (17p, 7,1n, 0,5l)	(19p, 22,1n, 1,3l) (25p, 15,1n, 1,8l) (20p, 17,1n, 1l) (24p, 27,1n, 1,4l) (27p, 10,1n, 1,0l) (22p, 12,1n, 0,6l)

Tabelle 2. *Pareto-Optima des PREsTiGE-Anwendungsfalls*

DOI: 10.2195/lj_Proc_schier_de_201610_01
URN: urn:nbn:de:0009-14-44770

5 Zusammenfassung und Ausblick

In diesem Artikel wurden die Themen Cloud-Computing, Privacy und die Optimierung von Geschäftsprozessen betrachtet. Neben der Definition der Themen wurden gesetzliche Regelungen, mögliche Realisierungen und Standards in den jeweiligen Bereichen vorgestellt. Des Weiteren wurde ein Konzept zum Schutz von Privacy-relevanten Daten in einer kollaborativen Cloud-Plattform in Form einer Architektur vorgestellt. Darauf aufbauend wurde ein Konzept für eine Erweiterung vorgestellt, mit welcher sich Handlungsempfehlungen in der Wahl des Prozessflusses nach eigenen Präferenzen erstellen lassen und wie diese Erweiterung in der vom Forschungsprojekt PREsTiGE entwickelten Architektur integriert werden kann.

Neben der Implementierung der Graph-basierten Optimierung aus Kapitel 4 in die in Abbildung 1 dargestellten Architektur müssen noch weitere Privacy-Faktoren berücksichtigt werden und use-case-spezifische Kostenanforderungen erstellt werden. Da die Auswahl des Prozessflusses in den meisten Fällen nicht von Experten durchgeführt wird, müssen die Methoden und Werkzeuge zur einfachen Formulierung und Auswahl eines Prozessflusses für die Logistik-Domäne im Konfigurator entwickelt werden.

Literaturverzeichnis

[BJR00] Boekhoudt, P.; Jonkers, H.; Rougoor, M.: Graph-based analysis of business process models: Mathematics and Computers in Business and Economics (MCBE 2000). Proceedings of the WSEAS International Conference, 2000.

[BR94] Brandstädt, A.: Graphen und Algorithmen. Vieweg+Teubner Verlag, Wiesbaden, 1994.

[BU08] Bundesamt für Sicherheit in der Informationstechnik (BSI): BSI-Standard 100-1, 2008.

[BU11] Bundesamt für Sicherheit in der Informationstechnik (BSI): Privacy Impact Assessment Guideline for RFID Applications (PIA).

[BU12] Bundesamt für Sicherheit in der Informationstechnik (BSI): Sicherheitsempfehlungen für Cloud Computing Anbieter. Mindestanforderungen in der Informationstechnik. Eckpunktepapier, 2012.

[Bu90]: Bundesdatenschutzgesetz. BDSG, 1990.

[Co16]: General Data Protection Regulation. GDPR, 2016.

[EP14] U.S. Environmental Protection Agency (EPA): EPA and NHTSA Adopt First-Ever Program to Reduce Greenhouse Gas Emissions and Improve Fuel Efficiency of Medium- and HeavyDuty Vehicles. https://www3.epa.gov/otaq/climate/documents/420f11031.pdf, 08.08.2016.

[EU95]: RICHTLINIE 95/46/EG DES EUROPAISCHEN PARLAMENTS UND DES RATES zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr: Amtsblatt der europäischen Gemeinschaften, 1995; S. 31.

[IKA+09] Itani, W.; Kayssi, A.; Chehab, A.: Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures: 2009 International Conference on Dependable, Autonomic and Secure Computing (DASC), 2009; S. 711–716.

[JÄ15] Jäger, M.: Hochsicher, kaum genutzt, völlig veraltet. PGP, 2015.

[JA84] Jaffe, J. M.: Algorithms for finding paths with multiple constraints. In Networks, 1984, 14; S. 95–116.

[JB05] Jutla, D. N.; Bodorik, P.: Sociotechnical Architecture for Online Privacy. In IEEE Security and Privacy Magazine, 2005, 3; S. 29–39.

[JSW+15] Jäger, B.; Selzer, A.; Waldmann, U.: Die automatisierte Messung von Cloud-Verarbeitungsstandorten. Datenquellen für eine Standortmetrik. In Datenschutz und Datensicherheit, 2015; S. 26–30.

[KR12] Krampe, H.: Grundlagen der Logistik. Einführung in Theorie und Praxis logistischer Systeme. HUSS-VERLAG GmbH, München, 2012.

[MI08] Microsoft Corporation: Privacy Guidelines for Developing Software Products and Services.

[MÖ99] Möhring, R. H.: Verteilte Verbindungssuche im öffentlichen Personenverkehr Graphentheoretische Modelle und Algorithmen. In (Horster, P. Hrsg.): Angewandte Mathematik, insbesondere Informatik. Vieweg+Teubner Verlag, Wiesbaden, 1999; S. 192–220.

[NI11a] NIST: The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology, 2011.

DOI: 10.2195/lj_Proc_schier_de_201610_01
URN: urn:nbn:de:0009-14-44770

[NI11b] NIST Computer Security Division: Guidelines on Security and Privacy in Public Cloud Computing, 2011.

[PC09] Pearson, S.; Charlesworth, A.: Accountability as a Way Forward for Privacy Protection in the Cloud. In (Hutchison, D. et al. Hrsg.): Cloud Computing. Springer Berlin Heidelberg, Berlin, Heidelberg, 2009; S. 131–144.

[PE09] Pearson, S.: Taking account of privacy when designing cloud computing services: 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing, 2009; S. 44–52.

[RCL09] Rimal, B. P.; Choi, E.; Lumb, I.: A Taxonomy and Survey of Cloud Computing Systems: 2009 Fifth International Joint Conference on INC, IMS and IDC, 2009; S. 44–51.

[SB15] Stahl, F.; Burgmair, S.: Bollwerk. Top 10 der Datenschutzrisiken in Webapplikationen. In iX, 2015; S. 76–79.

[SPS+15] Schier, A.; Schwarzbach, B.; Pirogov, A.; Franczyk, B.: inter-cloud architecture for privacy-preserving collaborative BPaaS.

[SSP+15] Schier, A. et al.: Cloud-Architektur für Privacy-Management in kollaborativen Logistikprozessen. In (Noche, B. Hrsg.): Tagungsband. 11. Fachkolloquium Logistik 30. September und 1. Oktober 2015. TuL - Lehrstuhl für Transportsysteme und -logistik Universität Duisburg-Essen, Duisburg, 2015.

[Ve48]:Allgemeine Erklärung der Menschenrechte, 1948.

[WA87] Warburton, A.: Approximation of Pareto Optima in Multiple-Objective, Shortest-Path Problems. In Operations Research, 1987, 35; S. 70–79.

[WE13] Welp, J.: Mit Recht in der Cloud. Cloud Computing bietet große Chancen – für Unternehmen aller Branchen. Aber: Der rechtliche Rahmen muss stimmen., 2013.

[WR] Wolf, M.-B.; Rahn, J.: Cloud Computing für Logistik 2. Akzeptanz und Nutzungsbereitschaft der Logistics Mall bei Anwendern und Anbietern. Fraunhofer Verlag, Stuttgart, 2013.

[ZYZ+12] Zhang, G. et al.: Key Research Issues for Privacy Protection and Preservation in Cloud Computing: 2012 International Conference on Cloud and Green Computing (CGC), 2012; S. 47–54.

Dipl.-Inf. (FH) Arkadius Schier, Research Assistant at the Software Engineering, Fraunhofer-Institute for Materialflow and Logistics IML since 2006. Arkadius Schier was born in 1981 in Loben, Poland. Between 2002 and 2006 he studied Technical Computer Science at the University of Applied Sciences and Arts in Dortmund.

Lucas Petrich, Student Assistant at the Software Engineering, Fraunhofer-Institute for Materialflow and Logistics IML. Lucas Petrich was born 1991 in Muenster, Germany. Between 2011 and 2016 he studied Applied Computer Science at the Technical University Dortmund.

Prof. Dr. Michael ten Hompel, born in Bergisch-Gladbach, Germany, in 1958, studied Electrical Engineering at RWTH Aachen and graduated from Witten/Herdecke University in 1991. In 2000, he joined the managing board of Fraunhofer Institute for Material Flow and Logistics in Dortmund (since January 2005: Managing Director) and became head of the Chair of Materials Handling and Warehousing at TU Dortmund University.

Address:
Fraunhofer-Institute for Materialflow and Logistics IML,
Joseph-von-Fraunhofer-Straße 2-4, 44227 Dortmund,
Germany

Dipl.-Inf. Björn Schwarzbach, Research Assistant at the Chair of Information Management. Björn Schwarzbach was born in 1983 in Leipzig, Germany. Between 2001 and 2011 he studied Computer Science and Physics at Leipzig University.

Prof. Dr. Ing. Bogdan Franczyk, Chair of Information Management, Leipzig University and Wroclaw University of Economics. Bogdan Franczyk was born 1955 in Lwowek Sl., Poland. He holds the chair of Information Management in Leipzig since 2002 and in Wroclaw since 2010.

Address:
Leipzig University,
Grimmaische Straße 12,
04109 Leipzig, Germany

Wroclaw University of Economics,
ul. Komandorska 118 / 1290,
53345 Wroclaw, Poland